J Intell Manuf (2019) 30:1111–1123
https://doi.org/10.1007/s10845-017-1315-5

Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods

Mingtao Wu[1] · **Zhengyi Song**[1] · **Young B. Moon**[1]

Received: 1 December 2016 / Accepted: 17 February 2017 / Published online: 23 February 2017

Abstract CyberManufacturing system (CMS) is a vision for future manufacturing systems. The concept delineates a vision of advanced manufacturing system integrated with technologies such as Internet of Things, Cloud Computing, Sensors Network and Machine Learning. As a result, cyber-attacks such as Stuxnet attack will increase along with growing simultaneous connectivity. Now, cyber-physical attacks are new and unique risks to CMSs and modern cyber security countermeasure is not enough. To learn this new vulnerability, the cyber-physical attacks is defined via a taxonomy under the vision of CMS. Machine learning on physical data is studied for detecting cyber-physical attacks. Two examples were developed with simulation and experiments: 3D printing malicious attack and CNC milling machine malicious attack. By implementing machine learning methods in physical data, the anomaly detection algorithm reached 96.1% accuracy in detecting cyber-physical attacks in 3D printing process; random forest algorithm reached on average 91.1% accuracy in detecting cyber-physical attacks in CNC milling process.

Keywords CyberManufacturing systems · Security · Additive manufacturing · Machine learning

Introduction

CyberManufacturing system (CMS) is a blueprint for future manufacturing systems where physical components are fully integrated with computational processes in a connected environment. The CMS is expected to yield benefits in cost, efficiency, and sustainability, by taking advantage of technologies such as Internet of Things, Cloud Computing, Fog Computing, Cyber-Physical System, Service-Oriented Technologies, Modeling and Simulation, Embedded Systems, Sensor Networks, Wireless Communications, Machine Learning, and Advanced Manufacturing Processes (Song and Moon 2016; Ren et al. 2015). Similar concepts and visions have been developed in different scopes and under different names such as "Industrie 4.0" by Germany, "Monozukuri" by Japan, "Factories of the Future" by EU, and "Industrial Internet" by GE, thus confirming the universal recognition of the importance of the CMS vision.

Particularly the openness of the Internet enhances manufacturing activities with additional capabilities in communication, information resources, storage, and computation. A result can be a manufacturing system possessing intelligent capabilities such as self-awareness, self-prediction, self-optimization, and self-configuration abilities (Ren et al. 2015). However, the very openness also enlarges the vulnerability, especially the attack surface for Manufacturing Systems as analyzed by following five layers.

In CMS, the system can be conceived by five layers as defined by Song and Moon (2016): User Layer, Application Interface Layer, Core Service Layer, Integrated Connection Layer and Physical Provider Layer. Each layer is distributed globally and connected to upper and lower layers via the Internet. Therefore, the attack surface of the whole CMS system is enlarged by the additional layers and Internet connections comparing to the traditional factories. For example, a malicious input could come from integrated connection layer as a malicious real-time controlling command that changes production schedules. Another example is when malicious input could orient from a person in the middle attack between customer layer and application interface layer

✉ Young B. Moon
ybmoon@syr.edu

[1] Department of Mechanical and Aerospace Engineering, Syracuse University, Syracuse, USA

as a maliciously altered file. Also, malicious input could exchange between different components in physical provider layer. If a manufacturing system is developed with the five layer CMS structure, security will be a critical concern for development and maintenance of CMS.

Currently even for other future manufacturing systems, security is becoming a critical concern. Ren et al. (2015) considers security as critical, especially for competitive enterprises under cloud manufacturing vision. Jazdi (2014) suggests that Industrie 4.0 brings many challenges including security needs to be extensively studied in the research. As suggested by Minnick (2016), indiscriminate internetworking is the biggest problem facing manufacturing today. The traditional methods such as firewalls are never enough, and intrusion detection takes time. For example, average intrusion takes more than two months to detect and even longer to remediate. Moreover, a recent study by IBM (2016) reports that manufacturing is the second most frequently targeted industry in 2015 in terms of the number of cyber-attacks.

The confidentiality, integrity, and availability, also known as the CIA triad, are important factors in dealing with security in CMS. The confidentiality includes SCADA (supervisory control and data acquisition) data security, preventive maintenance data security, customer personal information, etc. The integrity includes machine data integrity, production plan data integrity, source file integrity, etc. The availability includes machine availability, real-time control orders availability, customer user interface availability, etc. In CMS each factor influences differently in every layer, which is different from a traditional production environment that puts availability in the first priority.

In the next section, we propose and analyze a taxonomy of attacks in CMS systems, and define new and unique Cyber-Physical attacks. In section three, we present machine learning methods that were implemented on CMS environments for security. In section four, we provide two experimental results with machine learning methods detecting malicious attacks in 3D printers and CNC machines. A preliminary real-time detection system that was designed and implemented is also described.

Attacks in CyberManufacturing systems: a taxonomy

In order to clarify and classify attacks in CyberManufacturing systems, we implement taxonomy proposed by Yampolskiy et al. (2013) for describing cross-domain attacks in CMS.

Taxonomy

The taxonomy uses the distinction between *Influenced Element* and *Victim Element*. As a result, we can define following four categories of attacks: Cyber–Cyber attacks, Cyber-Physical attacks, Physical-Cyber attacks, and Physical–Physical attack (Fig. 1).

In *Cyber–Cyber attacks* category, influenced element and victim elements are in cyber domain, which is typical of cyber security problems. In cyber security, Cyber–Cyber attacks have been researched extensively thus are reasonably well understood. For example, denial-of-service (DoS) attack on the wireless communication over the factory floor network connecting sensors and actuators in CMS environments is a common Cyber–Cyber attack. The developed countermeasure and preventive techniques are firewall, access control, intrusion detection system, cryptography.

In *Cyber-Physical attacks* category, the influenced element is in the cyber domain, whereas victim element is in the physical domain. Currently, this category of attacks is the least understood one (Yampolskiy et al. 2013). A real example from critical infrastructure security is Stuxnet, which is known for destroying roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control (Kelley 2013).

In *Physical-Cyber attacks* category, the influenced element is in the physical domain, whereas victim element is in the cyber domain. This effect of propagation has been studied within the embedded system security (Yampolskiy et al. 2013). One Physical-Cyber attack is by monitoring acoustic signal emanations of typing a keyboard, recovering the keystroke from a victim and resulting in cyber information leakage such as password (Zhu et al. 2014).

In *Physical–Physical attacks* category, both influenced element and victim element are in the physical domain. For example, a malicious infotainment systems make the vehicles vulnerable remote attack (Zetter 2015a). In this case, the influenced element is car's infotainment system, and the victim element is the car's physical components. Another example shows that researchers can build "back door" software into hardware and it is almost undetectable (Zetter 2015b). Such malicious hardware is built intendedly or unintendedly by suppliers and form Physical-Physical attacks in CMS systems, and cause unsafe and insecure products for customers.

Overall, the Physical-Physical attack is a comparatively well-understood area (Yampolskiy et al. 2013). Standards such as ISO 9000 series for quality management and ISO/IEC 27001:2013 as information security standard can help manufacturers select suppliers.

Cyber-physical attacks: the new vulnerability

The Cyber-Physical attack is a new but unique risk in the cyber-physical environment, such as smart grid, CMSs, connected vehicles, etc.

In 2010, Iranian secret centrifuges was targeted by Stuxnet computer worm. On the infected machines, the centrifuges

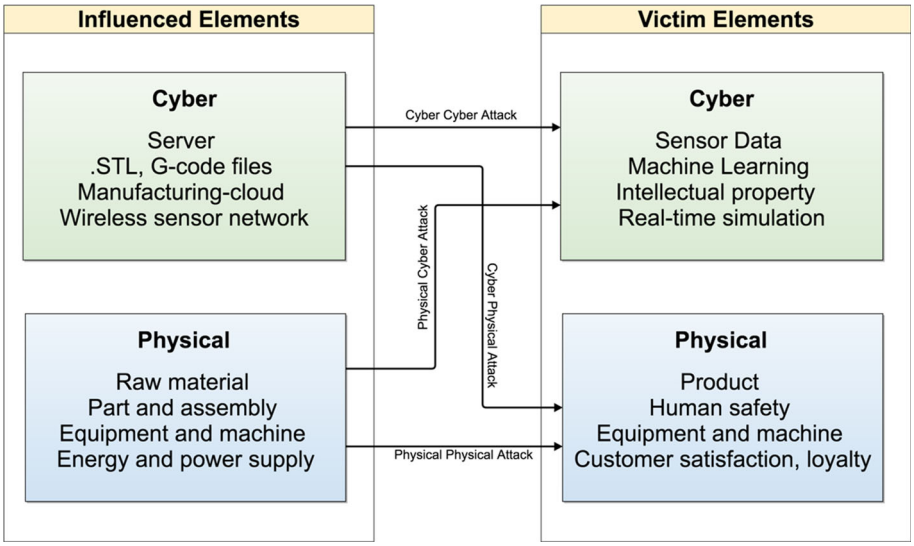

Fig. 1 Taxonomy of attacks in CyberManufacturing systems

can be maliciously speeded up or slowed down and finally get destroyed. For the first time, Stuxnet showed its ability on cyber-physical attacks.

In 2015, an unnamed steel mill in Germany was attacked. According to a report, hackers manipulated the control system that a blast furnace could not be properly shut down, resulting in unspecified "massive" damage. This is the second confirmed case of a cyber-physical attack that cyber-attack caused physical destruction of equipment (Zetter 2015a), after the Stuxnet case.

In 2015, an airplane on-board entertainment system was taken control by a security researcher in the airplane. The researcher claimed that he was able to issue a climb command and make the plane briefly change course (Zetter 2015b). Later in 2015, two hackers demonstrated that they could remotely control a Jeep Cherokee's ignition switch, brakes and steering system (WIRED 2015). All examples above are cyber-physical environments attacked by cyber-physical attacks.

Cyber-physical attacks in CMS environment

To better understand Cyber-Physical attack, we define it as following:

The attacks initiate inside or outside CMS environment as *digital* format and intrude via *cyber*, causing *physical* components such as machines, equipment, parts, assemblies, products have over wearing, breakage, scrap or any other change that original design not intend to be.

In manufacturing systems, Cyber-Physical attacks start to cause concern. Wells et al. (2014) designed an experiment on CNC milling machines infected with a virus, which altered the tool path file. The result showed 19% loss in performance. Turner et al. (2015) conducted a experiment to test participants' awareness of cyber-attack in manufacturing with virus rewriting the G-Code to alter the part's geometry for a 3D printer. The result shows that of the seven groups, none identified a malicious entity corrupting the file. Sturm et al. (2014) proved a maliciously defected 3D printed part could reduce yield load by 14%. The malicious defect is a void placed inside of a part, causing a failure of an ASTM Standard D638-10 tensile test specimen. Zeltmann et al. (2016) provided an overview and evaluated the potential risks that exist in the cyber-physical environment with additive manufacturing.

Cyber-Physical attack can affect the physical performance of a machine, equipment or component in manufacturing system, causing change in shape, weight, structural stiffness, natural frequency, etc. of a part. Those changes could result in defective parts, assembly mistakes, tool breakage, over wearing and unqualified products.

Due to the uniqueness of cyber physical attacks, detection cannot merely rely on network countermeasures. Vincen et al. (2015) proposed a side channel analysis based on Structural Health Monitoring (SHM) detecting malicious defects in manufacturing systems. Different from Vincent's work, this research focuses on the manufacturing process other than just finished part, thus can prevent defective parts in an earlier stage. Moreover, this research uses two different manufacturing process (3D printing and CNC milling) to explore and demonstrate the need for new methods for detecting attacks cyber-physical attacks in manufacturing systems.

The unique Cyber-Physical attacks bring up challenges to CMS: (i) the sabotage can be executed remotely via the Internet access, which is ubiquitous in CMS environment; (ii) comparing to office IT security, the loss of 24/7/365 availability in CMS leads to direct disorders in production systems, especially in realms such as real-time control and simulation; and (iii) cyber security countermeasures that focus on office IT security having left blind-spots for detecting attacks in CMS factory floor.

Cyber-physical attack detection: data and machine learning

To detect cyber physical attacks in a manufacturing environment, both cyber and physical detection methods should be used. The modern cyber-attack detection systems monitor either host computers or network links to capture cyber-attack data (Karthikeyan and Indra 2010). The cyber security approaches such as Intrusion Detection Systems (IDS), Misuse Detection/Misbehavior Detection Misuse, Signature based Approach, Anomaly Detection should be implemented on CMS computer and network environments. However, in a modern network environment, an intrusion detection could take months, which is not acceptable for the availability requirement for CMS production needs. Physical detection is necessary to complement the cyber detection. Fortunately compared with office IT network, manufacturing environment is more stable, easy to define rules and collect training data. Each machine has its own safe range and every part has its own manufacturing routine. Effective detection on physical data with machine learning can enhance the overall effectiveness.

Machine learning

Machine learning has been intensively applied both in physical security data and manufacturing system, but not in manufacturing security so far. Physical security data needed for machine learning can come from voice recognition, fingerprint authentication, gait authentication, keystroke and other biometrics (Jain et al. 2004). Machine learning implementations in manufacturing includes real-time vision system for surface defect detection (Jia et al. 2004), weld defect defection (Shen et al. 2010), surface defect detection (Zhang et al. 2011), preventative maintenance, supply chains optimization, etc.

The integration of cyber security and physical data machine learning is an approach to detect cyber-physical attacks. It can effectively enhance the accuracy and shorten the respond time. The cyber security approaches have been intensively researched in the past and can be implemented with IT security professionals. At the same time, the machine learning approach utilizing physical data can filter the false alerts from cybersecurity aided by domain experts from manufacturing.

Supervised learning: classification

Classification is a supervised machine learning method with the purpose of categorizing data sets. In machine learning, classification is implemented with various algorithms, also known as classifier, such as Support Vector Machine (SVM), C4.5 decision tree, artificial neural network (ANN), k-Nearest Neighbors, etc. Data sets for classification are pre-processed and analyzed to features. The process to define feature is a key process to enhance accuracy in machine learning results, called feature extraction which requires domain knowledge with data mining experience.

In this research, image and acoustic classifications have been used to detect malicious attacks in CMS processes. Random forest, k-nearest neighbors (kNN) machine learning algorithms have been implemented. *k-Nearest Neighbors (kNN)* classifier is used to perform discriminant analysis when reliable parametric estimates of probability densities are unknown or difficult to determine (Peterson 2009). *A random forest multi-way classifier* consists of a number of trees, with each tree grown using some form of randomization. The leaf nodes of each tree are labeled by estimates of the posterior distribution over the image classes. Each internal node contains a test that best splits the space of data to be classified (Bosch et al. 2007). In this research, three decision trees are used and each of them has five leaf nodes to classify (Wu et al. 2016). Compared to C4.5 decision tree algorithm, the random forest classifier achieves higher accuracy with relatively shorter time to execute.

Unsupervised learning: anomaly detection

Anomaly detection can identify abnormal behavior on a host or network (Kim et al. 2013), image (Chandola et al. 2009), supervisory control and data acquisition (SCADA) (Garcia et al. 2011), or for equipment preventive maintenance (Rabatel et al. 2011). It refers to the problem of finding patterns in data that do not conform to expected behavior (Chandola et al. 2009). The principle is to recognize patterns of accepted behavior, which is learned or specified by the algorithm. Activities that fall outside the predefined or accepted model of behavior will alert administrators. The advantage of anomaly detection is that it can detect novel attacks comparing to supervised approaches. However, the disadvantage of network anomaly detection is the difficulty in defining rules for normal network behavior.

Since it is impossible to predict every possible attack that a hacker may try against CMS system, the anomaly detection method is combined with the random forest method to increase the accuracy in this research.

The data captured from 3D printing and CNC milling processes are pre-processed for anomaly detection with features extracted according to different process characters.

Based on the data, the random forests algorithm is used to build the process-based patterns. With the built patterns, outliers are detected according to different features used in the process. Once such outliers are detected, the system sends out alerts.

The anomaly detection algorithm finds intrusions by spotting unusual activities or outliers. There are three potential

Table 1 CMS process attacks analysis and data extraction

Process	Attack aim	Symptom	Consequence	Detection data
3D printing	Design infill nozzle travels speed heating temperature	Hidden void surface gap high energy consumption	Scrap parts overheating	Vision energy consumption acoustic
CNC milling	Design spindle speed feed speed	Change in vibration change in chip shape cutting bit temperature tool breakage	Scrap parts overwear tool breakage overheating	Acoustic temperature time

outliers in 3D printing process: (1) increase in the mean value of image greyscale value over the malicious defects area, (2) increase in the standard derivation of image greyscale value, (3) increase in the number of pixels that greyscale value higher than a threshold. There are also three potential types of outliers in the CNC milling process: (1) increase in the mean value of amplitude, (2) increase in the standard derivation of amplitude, (3) increase in the number of points amplitude larger than threshold.

The random forests algorithm uses proximities to find outliers whose proximities to all other cases in the entire dataset are generally small. The average proximity from case n in class j to case k (the rest of data in class j) is computed as function (1):

$$\overline{\mathrm{P}}(\mathrm{n}) = \sum\nolimits_{class(k)=j} prox^2(n,k) \tag{1}$$

The raw outlier-ness of case n is defined as $N/\mathrm{P}(n)$ where N stands for the number of cases in the data set. For each class, the median and the absolute deviation of all raw outlier-ness are determined. The median is subtracted from each raw outlier-ness. The result of the subtraction is divided by the absolute deviation that gives the final outlier-ness. If the outlier-ness of a particular case is large and the proximity is small, the case is considered to be an outlier (Prashanth et al. 2008).

Data in CMS environment

To implement machine learning in CMS security, data/signal processing and feature selection and extraction are key steps. Data sources can be used including vision, acoustic, energy, temperature, weight, etc. Some of the data can be directly drawn from controlling system whereas others need additional monitoring systems.

Collection and processing

CMS processes can consist of traditional and advanced manufacturing processes. They include additive manufacturing, subtractive manufacturing, molding, forming, joining, casting, coating, high-speed assembly and others. In this research, we use 3D printing and CNC milling processes as two examples.

To decide what data to extract from the manufacturing process for security purposes, the following factors should be analyzed: (i) what is the process and what is the attack aim, (ii) what is the symptom and consequence, and (iii) what data can be collected from the machine for detection.

3D printing is a key enabling technology for CMS. It is getting extensively popular in recent years, and some new machines are developed with wireless network capability, which also increases the attack surface for a successful attack. The attack aims for 3D printing could be: change the design dimensions, change the infill with malicious void, change nozzle travel speed, or change heating temperature. The symptom could be quite implicit, such as a hidden void, surface gap or high energy consumption, and finally, leads to scrap parts. For 3D printing, vision, acoustic and energy consumption could be potential features.

Computer Numerical Control (CNC) milling process is a representative process for subtractive manufacturing process. The attack can aim for CNC milling process to alter design, spindle speed, or feed speed. The design change can create scrap parts. The increase in spindle speed can expedite the tool wear. Also, the increase in feed speed can break cutting tools. For CNC milling, acoustic, temperature and time can be potential features (Table 1).

Feature extraction

For machine learning in manufacturing, feature extraction is a critical process. It starts from an initial set of measured data and builds derived values (features) intended to be informative and non-redundant, facilitating the subsequent learning and generalization steps, and in some cases leading to better human interpretations https://en.wikipedia.org/wiki/Feature%20extraction. A feature is a good data representation of a symptom, phenomenon or measurement. For example, high value of acoustic emission during drilling process can mean wrong spindle speed or wrong part material. The feature extraction process requires domain knowledge and data processing experience.

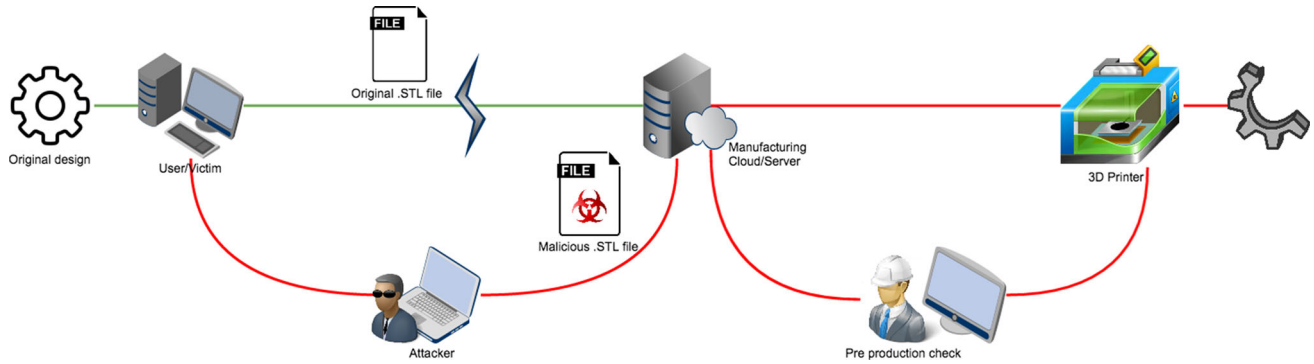

Fig. 2 Man-in-the-middle attack for a cyber-based 3D printing process

Simulation of attack detection in CMS processes: two examples

Two examples were developed to test and demonstrate how machine learning methods can be utilized in CMS security. In "Additive Manufacturing process: a 3D printing example" section, we present an experiment design of detecting malicious defects in 3D printing process using machine learning with image data. In "Subtractive manufacturing process: a CNC milling example" section, we present an experiment design of detecting malicious defects in CNC milling process using machine learning with acoustic signal data.

Additive manufacturing process: a 3D printing example

3D printing, or additive manufacturing, is a key technology for advanced manufacturing systems (Wu et al. 2016). However, 3D printing systems have unique vulnerabilities presented by the ability to affect internal layers without affecting the exterior layers (Sturm et al. 2014). By changing design or dimensions in the ".STL" file, malicious defective parts could be manufactured without any prior alert.

Attack mode

Man-in-the-middle attacks can easily accomplish the process of replacing a original ".STL" file with a malicious design ".STL" file. As shown in Fig. 2, during the user's uploading original ".STL" file to manufacturing server to put an order, an attacker can alter the communication between user and server, and replace with malicious ".STL" file.

If a hacker designed a malicious infill void defect that cannot be observed from the surface of the final product, the part will be manufactured without noticing any abnormalities. During the pre-production check process, operators cannot detect the difference between the original design and malicious design because the malicious design can be implicit. The malicious file will then be sent to 3D printers and the finished defective parts will be sent to the customers. As shown by Sturm et al. (2014), the void in a 3D printing part will result in reduction of yield, with other corresponding physical characteristic changes such as weight, stiffness and natural frequency.

Five different infill defect patterns were designed as shown in Fig. 3: seam, irregular polygon, circle, rectangle, and triangle to simulate attacks. The examples illustrated in Fig. 3 are parts with 10% honeycomb infill.

Data collection: image simulation and experiment

Images were captured from the 3D printing software MakerBot Desktop 3.9.1 preview function. The size of images is 512 × 512 pixels. The selection of image size was done in considering feature extraction process.

In total, 3887 simulation images were generated for simulation. 532 images of non-defect parts were captured, labeled as group A. The non-defect group A images were captured every 2–4 layers during the printing process, with infill density varied from 8–12% to increase the diversity of the training images. 3355 images of defective parts were captured and labeled as group B. The defective group B images were captured every 2–4 layers during the printing process, with combinations of 5 different defects. The infill density is 10% for group B.

Another method used in images collection is to capture real images during printing process with mini cameras attached on 3D printer structures. To test and verify the image classification method in real environment, a camera-based vision detection system has been designed and installed on MakerBot Replicator^{TM}2. MakerBot Replicator^{TM}2 has the building envelope of 11.2 × 6.0 × 6.1" and can print at 100 μm per layer. Installation of the camera on a MakerBot Replicator 2 is shown in Fig. 4. In this work, we developed two ways to install on MakerBot Replicator 2. One is mounting the camera right next to the intruder and move along with it, called 'moving camera.' The other is mounting the cam-

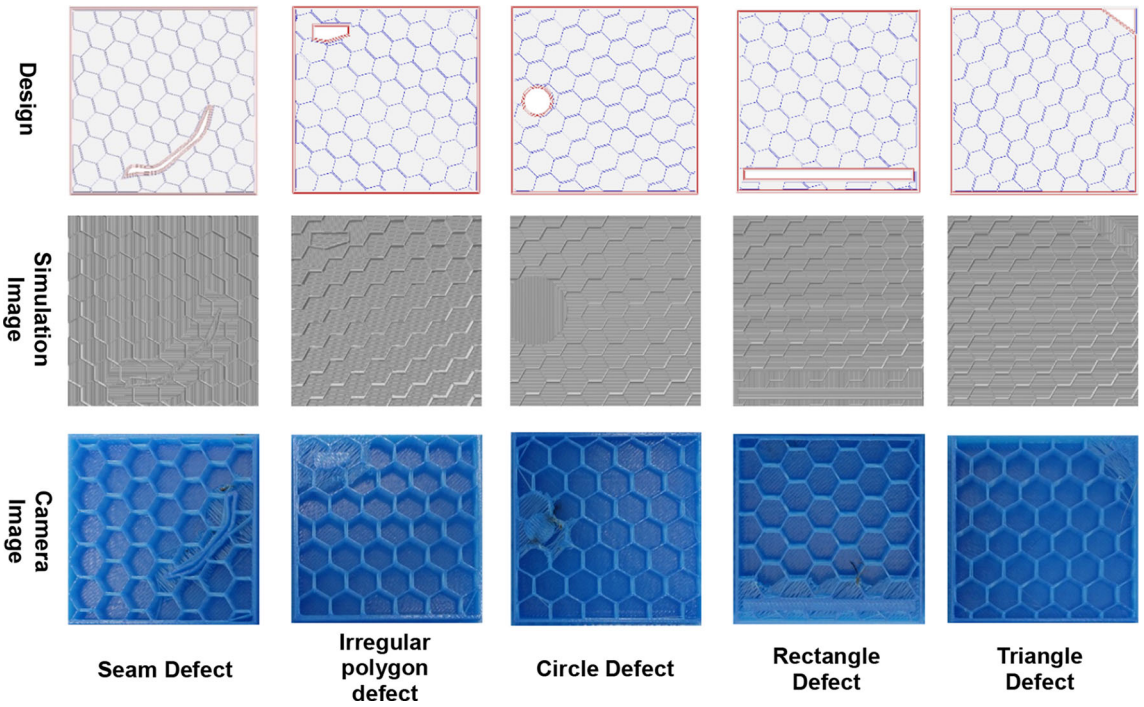

Fig. 3 Malicious defect designs, simulation images and camera images

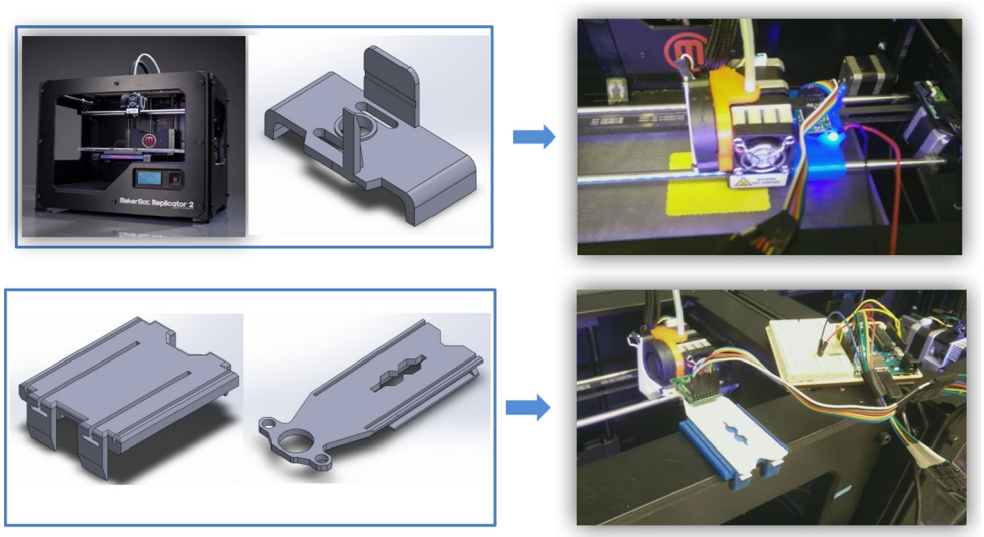

Fig. 4 MakerBot replicator 2 printer with moving camera and static camera

era on the frame of the 3D printer, called 'static camera.' The 'static camera' can capture clear image and reach higher accuracy. The 'moving camera' should have same accuracy and can adapt to more conditions, without the blurring caused by motion.

The camera is an Arducam Mini Module Camera Shield with OV2640 2 Megapixels Lens, compatible with Arduino UNO Mega2560 Board. The camera unit dimensions are $3 \times 2 \times 1$ inches, connected to the Arduino UNO via extended jumper wires. With programming in Arducam software, it can produce images any size scaling down from SXGA to 40×30 in jpeg format. As a result, the feature extraction process for previous 512×512 size images needed to be altered.

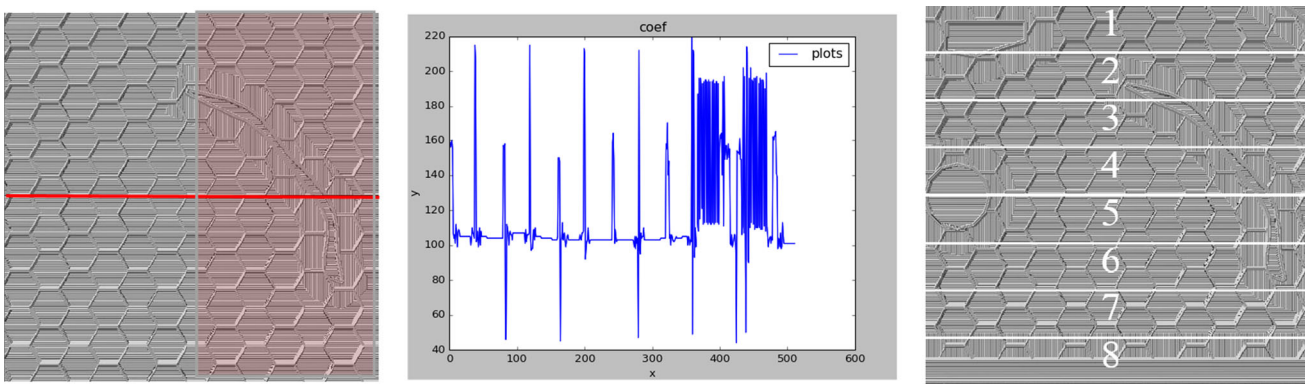

Fig. 5 Grayscale plot row no. 250, section separation

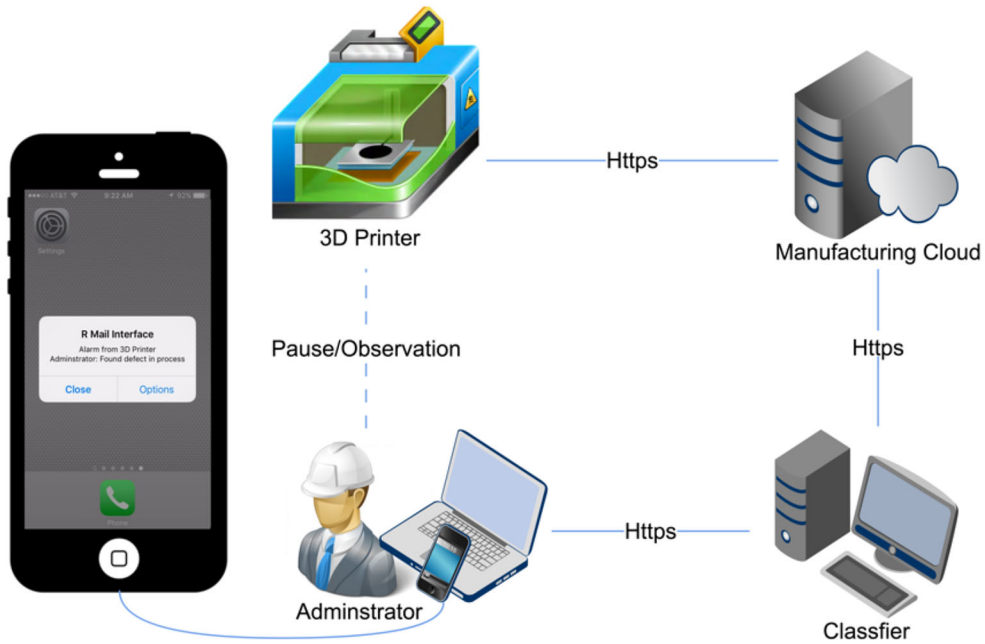

Fig. 6 Preliminary wireless real-time alert system for 3D printing process

Feature extraction

The feature extraction process was implemented in R and RStudio Desktop.

By plotting simulated image row No. 250 (marked in red in Fig. 5) grayscale value, we can observe repetitive peaks in normal area on the left, one medium peak followed by one high peak, in pairs. In defective area on the right, the greyscale plot shows constant volatility. To specify peaks, we set threshold of grayscale at 120.

For feature extraction, each image is equally divided into eight sections as shown in Fig. 5. Each section contains 64 rows, 32,768 pixels. The following features are extracted for defect classification.

- Mean of grayscale in each section.
- Standard derivation of grayscale in each section.
- Number of pixels grayscale larger than 120.

As a result, every image has 24 features, from eight sections, each section provides three features (Wu et al. 2016).

Three machine learning algorithms are used in detecting malicious defect: k-Nearest Neighbors (kNN), random forest and anomaly detection.

Real-time detection

A prototype system was designed and connected to 3D printer and computers. As shown in Fig. 6, it is designed to send real-time alert to administrator indicating malicious defect. The vision system on 3D printer is connected to Internet via Raspberry Pi B+. The camera is updated with Raspberry Pi OV 5647 Camera To be compatible with Raspberry Pi B+, and also improve the image quality.

Table 2 3D printing process accuracy results

Accuracy		Machine learning method		
		Random forest (%)	kNN (%)	Anomaly detection (%)
Image from simulation	Honeycomb	88.4	81.3	100.0
	Diamond	100.0	85.0	100.0
	Linear	94.6	92.5	100.0
	Star	97.8	100	99.8
	Catfill	91.5	100	100.0
Image from moving camera	Honeycomb	68.4	68.75	72.5
Image from static camera		95.5	87.5	96.1

Raspberry Pi B+ is used as the mini-computer system to connect to the network wirelessly and operate the Raspberry Pi OV5647 Camera to capture images of the printed object at a set time interval. Once the images are captured and saved to the Pi, BitTorrent Sync is used to synchronize the images from the device to the cloud service. The computer with classifier testing real-time collected images. If detected any malicious defects, the program will send an alert to the user via text message and email. As shown in Fig. 6, the email says "Alert from 3D printer, Administrator: Found defect in process".

An experiment was conducted during a 3D printing process under attack. After testing, the whole process can be accomplished within 1 min, including the time for syncing and downloading images (largely depend on server and Internet speed) and feature extraction and classify time (within few seconds), and a real-time alert is send to an operator via mail system.

Result analysis

The goal of this experiment is using machine learning and physical data from cameras to detect malicious defects. The accuracy of machine learning results is one of the measurements for effectiveness of the system. The machine learning accuracy is defined by the Eq. (2). Where *TruePositive* means images in class A that are predicted as class A, and *TrueNegative* stands for images in class B predicted as class B.

$$\text{Accuracy} = \frac{\text{TruePositive} + \text{TrueNegative}}{\text{Total}} \tag{2}$$

Moreover, the compatibility of the system is also tested by running with 5 different infill shapes of 3D printing process: Honeycomb, Diamond, Linear, Star, Catfill. Finally, the system effectively under real environment comparing to simulation is analyzed.

As shown in Table 2:

Table 3 Simulation signal parameters

Parameter	Value
Fundamental frequency	40 Hz
Harmonic frequency	80, 120, 160, 320 Hz
Normalized amplitude	0.3 for milling exterior boundaries 1 for milling interior boundaries
White noise	$0.1 \times N(0,1)$
Acquisition frequency	100 Hz

(1) Anomaly detection is most accurate method among three chosen methods in detecting malicious defects. Accuracy is 96.1% which is acceptable for the experimental result and can be improved by refinement in hardware and software.
(2) Based on simulation images experiment, the different types of infill have a minor influence on system accuracy, but not critical.
(3) Camera images have lower accuracy compared to simulated images. Among camera images, moving camera's final accuracy 72.5% is not acceptable because of the blur created by motion. Static camera images have a better accuracy of 96.1%, thus proves the system effectiveness in a real environment.

Subtractive manufacturing process: a CNC milling example

CNC machining is a typical subtractive processing. During the decades, CNC has been core manufacturing units in manufacturing systems. The flexibility and automation of manufacturing systems have been significantly enhanced by implementation of CNC machining. Since CNC processing could be totally manipulated by programming, it shows its vulnerability towards cyber-physical attacks.

Attack mode

By implementing man-in-the-middle attack, attackers can replace original G-code designs with malicious G-code. Two attack scenarios have been developed as a result of malicious codes.

Scenario 1: Attack on Design

The first attacking scenario is to alternate the positioning parameters during processes and therefore change the profiling routine of tools. As a result, the geometric design will change. The change in tool path could cause assemble mistakes, structural weaken and possibly breakage. As shown in Fig. 7, edge 2–3, 4–5, 5–6 and 6–7 offset inward the contour.

Scenario 2: Attack on Operation

The second attack mode proposed in this research is the change in machining operation parameters. In this section, a change in spindle speed in milling operation is captured for further research. In real case, fast rotation speed can cause over wear of tool; a tool with too slow rotation will risk in being broken by shear force in the feeding direction. In the scenario, spindle speed is maliciously altered from 1200 to 2000 rpm.

Data collection: acoustic signal simulation and experiment

Acoustic signal is selected as the index to detect any malicious change in CNC milling process. Similarly, both simulation and experiment methods are adopted for testing.

Simulated signal is a time-serial amplitude numbers, created by a summation of sine-functions with fundamental frequency, harmonic frequencies and a Gaussian noise. The advantage of adopting simulated signal in this scenario is to enhance variety of signals for test and analysis with more parameters setting, and generate enough data for further analysis. The parameter used for acoustic signal generation are listed in Table 3, and the simulated signals were generated in R.

The experiments were conducted on a CNC machine Bridgeport Milling Ez-trak. The milling tool is a 2-flute, 3/16 end mill with rotation speed of 1200 rotation per minute. The material of work piece was aluminum. Moving speed of the tool was 10 inch per minute. Feed rate was 50/1000 of 1 inch for the first six milling cycles, 20/1000 of 1 inch for the last cycle.

According to Duro et al. (2016); Song et al. (2017), microphone provides the best balance in satisfying the many requirements of a sensor for recording acoustic signal in milling operations. Three microphones from smartphones: iPhone 5s microphone, iPhone 6s plus microphone and iPhone 6s with ear pod microphone were implemented as the acoustic sensors to recording signals.

The sample part is designed as Fig. 8.

Feature extraction

The monitored signals were digitalized by MATLAB software. All the sound signal data were pre-processed by sectioning the whole period into sound periods of each individual cycle. In order to increase the number of the training data set, the real sound signal data were also sampled by 10 observations each. R was used for machine learning programming. The packages used for sound wave editing and analysis are "tuneR" and "seewave". The packages used for machining learning detection and analysis are "randomForest", "h2o" and "pROC" (Song et al. 2017) (Fig. 9).

According to the simulated and recorded signal, three key feature is selected.

- Mean of amplitude in each period of time.
- Standard derivation of amplitude in each period of time.
- Number of points amplitude larger than threshold.

In experiment, period of time is set as 80 s, threshold for simulation is set as 1000, threshold for experiment signal is set as 2.5.

Similar to "Additive manufacturing process: a 3D printing example", three machine learning algorithms are used in detecting malicious defect: kNN, random forest and anomaly detection. The real time synchronizing system can be implemented as "Real-time detection".

Result analysis

Accuracy is the key measurement for detecting effectiveness as defined in "Result analysis". The results of detecting malicious defects in CNC milling process via acoustic signal shown as Table 4.

As shown in Table 4,

(1) Anomaly detection and random forest method hold high accuracy for both scenario 1 and 2 in simulated signal, and scenario 2 in real signal. In real signal, the random forest shows highest average accuracy of 91.1%.
(2) Scenario 1 shows a slightly lower prediction accuracy comparing to scenario 2.
(3) Real signal has lower accuracy in scenario 1 than simulated signal, the reason could be the background noise from recording environment, and also the complexity of scenario 1 attack mode.

Conclusion

Cyber-Physical attacks are unique but critical for security in CyberManufacturing Systems. Modern cyber security countermeasures are not sufficient in handling security issues

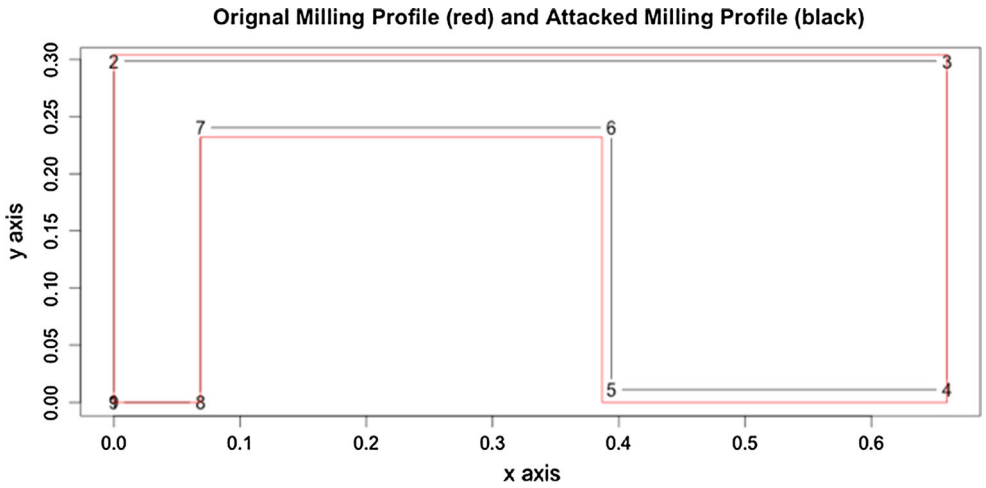

Fig. 7 Comparison of original and attacked milling profiles

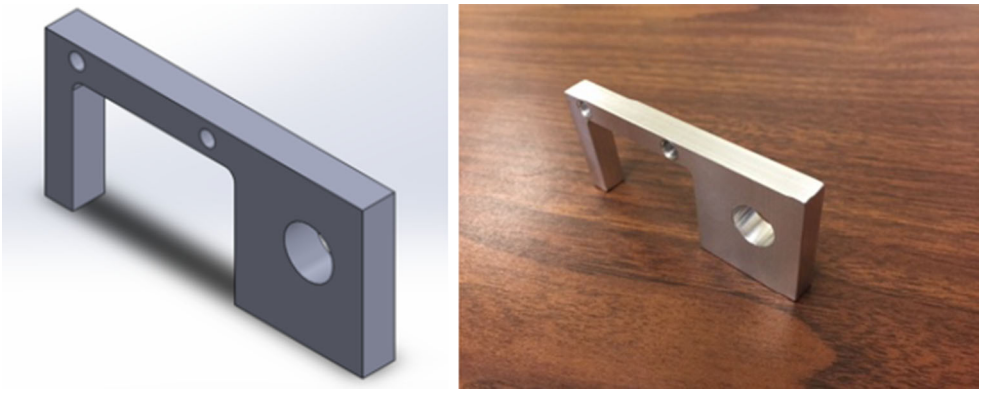

Fig. 8 Sample part

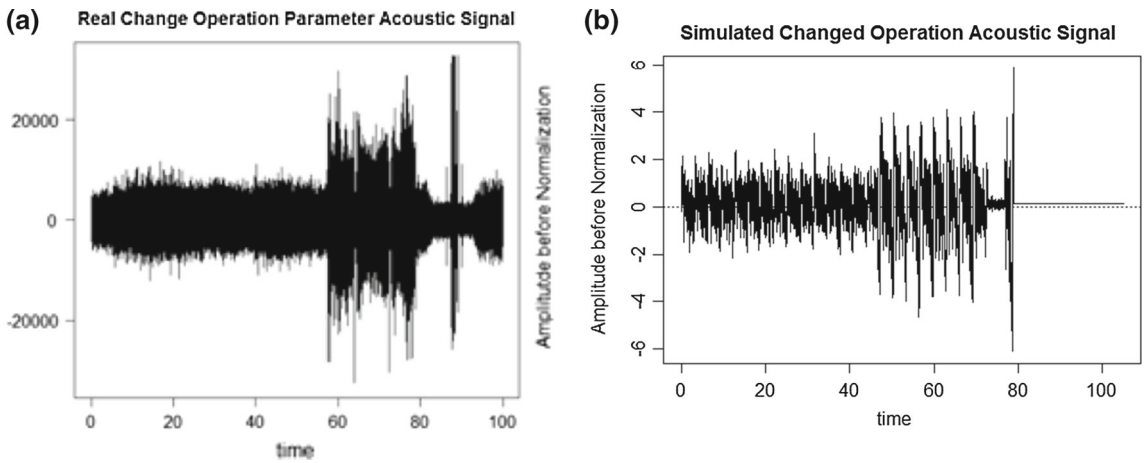

Fig. 9 Plot of sound wave in attacked scenario 2. **a** Real changed operation signal, **b** simulated changed operation signal

in CMS. In this research, physical data machine learning approaches are developed and integrated for detecting Cyber-Physical attacks in CMS.

We developed two examples with simulation and experimentation to test and demonstrate the physical data machine learning security approach. In the 3D printing process example, we used vision as physical data source for machine learning. Three different machine learning algorithms are implemented with image classification. The anomaly detection method returned the highest accuracy of 96.1% in

Table 4 Machine learning accuracy for CNC milling process

Accuracy		Machining learning method		
		kNN (%)	Random forest (%)	Anomaly detection (%)
Simulated signal	Scenario 1	50	93.1	93.8
	Scenario 2	50	100	100
Real signal	Scenario 1	70	82.2	79.6
	Scenario 2	77.8	100	100

detecting a malicious defect in printing process. In the CNC milling process example, we design two attack modes in changing the part design and manufacture operation. Acoustic signal is selected as source of physical data for machine learning process. Same three different machine learning algorithms were implemented with the random forest algorithm returned the highest average accuracy of 91.1%

Detecting cyber-physical attacks in CMS environment is not easy and needs further research. For more future work, (i) research on more manufacturing processes and match with suitable detection methods and data process; (ii) extract more than one category of data in 3D printing and CNC milling process to enhance detecting accuracy, (iii) Detection on manufacturing processes with malicious defects integrated in a system. (iv) development of cyber-physical environment security policy, security standards, product design for security, security framework for CMS.

References

Bosch, A., Zisserman, A., & Munoz, X. (2007). Image classification using random forests and ferns. In *2007 IEEE 11th international conference on computer vision*, pp. 1–8.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection. *ACM Computing Surveys*, *41*(3), 1–58.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computig Surveys*, *41*(3), 1–58.

Duro, J. A., Padget, J. A., Bowen, C. R., & Kim, H. A. (2016). Multi-sensor data fusion framework for Cnc machining monitoring. *Mechanical Systems and Signal Processing*, *67*, 505–520.

Garcia, R. F., Rolle, J. L. C., & Castelo, J. P. (2011). A review of SCADA anomaly detection systems. *Advances in Intelligent and Soft Computing*, *87*, 405–414.

IBM (2016). *Reviewing a year of serious data breaches, major attacks and new vulnerabilities*.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20.

Jazdi, N. (2014). Cyber physical systems in the context of industry 4.0. In *Automation, quality and testing, robotics. 2014 IEEE* , pp. 2–4.

Jia, H., Murphey, Y. L., Shi, J., & Chang, T. S. (2004). An intelligent real-time vision system for surface defect detection. *Proceedings—International Conference on Pattern Recognition*, *3*(February), 239–242.

Karthikeyan, K. R., & Indra, A. (2010). Intrusion detection tools and techniques–A survey. *International Journal of Computer Theory and Engineering*, *2*(6), 901–906.

Kelley, M. B. (2013). The Stuxnet attack On Iran's nuclear plant was 'Far More Dangerous' than previously thought. *Business Insider*. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Kim, A. C., Park, W. H., & Lee, D. H. (2013). A study on the live forensic techniques for anomaly detection in user terminals. *International Journal of Security and Its Applications*, *7*(1), 181–187.

Minnick, J. (2016). *The Biggest Cybersecurity problems facing manufacturing in 2016*. http://www.mbtmag.com/article/2016/01/biggest-cybersecurity-problems-facing-manufacturing.

Peterson, L. (2009). K-nearest neighbor. *Scholarpedia*. http://www.scholarpedia.org/article/K-nearest_neighbor. Accessed June 23, 2016.

Prashanth, G., Prashanth, V., Jayashree, P., & Srinivasan, N. (2008). Using random forests for network-based anomaly detection at active routers. In *2008 International conference on signal processing communications. Networking, 2008*, pp. 93–96

Rabatel, J., Bringay, S., & Poncelet, P. (2011). Anomaly detection in monitoring sensor data for preventive maintenance. *Expert Systems with Applications.*, *38*, 7003–7015.

Ren, L., Zhang, L., Tao, F., Zhao, C., Chai, X., & Zhao, X. (2015). Cloud manufacturing: From concept to practice. *Enterprise Information Systems*, *9*(2), 186–209.

Shen, Q., Gao, J., & Li, C. (2010). Automatic classification of weld defects in radiographic images. *Insight Non-Destructive Testing Condition Monitoring*, *52*(3), 134–139.

Song, Z., & Moon, Y. B. (2016). Performance analysis of CyberManufacturing systems?: A simulation study. In *13th IFIP international conference on product lifecycle management*.

Song, Z., Zhou, H., Cheung, J., & Lin, L. L. (2017). Detecting attacks in CyberManufacturing systems?: Subtractive manufacturing example. In *International conference on manufacturing technologies*, pp. 1–4.

Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., & Parker, R. (2014). Cyber-physical Vunerabilities In *Additive manufacturing systems, in international solid freeform fabrication symposium proceedings*, pp. 951–963.

Turner, H., White, J., Camelio, J. A., Williams, C., Amos, B., & Parker, R. (2015). Bad parts: Are our manufacturing systems at risk of silent cyberattacks? *IEEE Security & Privacy*, *13*(3), 40–47.

Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. *Procedia Manufacturing*, *1*, 77–85.

Wells, L. J., Camelio, J. A., Williams, C. B., & White J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), 74–77.

WIRED (2015). Hackers remotely kill a jeep on the highway. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed May 03, 2016.

Wu, M., Phoha, V. V., Moon, Y. B., & Belman, A. K.(2016). Detecting malicious defects in 3d printing process using machine learning and image classification. In *Proceedings of the ASME 2016 international mechanical engineering congress and exposition*, pp. 4–9.

Wu, M., Zhou, H., Lin, L. L., Silva, B., Song, Z., Cheung, J., & Moon, Y. (2016). Detecting attacks in CyberManufacturing systems?: Additive manufacturing example. In *International conference on mechanical, materials and manufacturing*, pp. 1–5.

Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2013). Taxonomy for description of cross-domain attacks on CPS. In *Proceedings of the 2nd ACM international conference on high confidence networked systems*, pp. 135–142.

Zeltmann, S. E., Gupta, N., Tsoutsos, N. G., Maniatakos, M., Rajendran, J., & Karri, R. (2016). Manufacturing and security challenges in 3D printing. *Jom*, *68*(7), 1872–1881.

Zetter, K. (2015). A cyberattack has caused confirmed physical damage for the second time ever. In *WIRED*. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

Zetter, K. (2015). Feds say that banned researcher commandeered a plane. In *WIRED*. https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

Zhang, X. W., Ding, Y. Q., Lv, Y. Y., Shi, A. Y., & Liang, R. Y. (2011). A vision inspection system for the surface defects of strongly reflected metal based on multi-class SVM. *Expert Systems with Applications*, *38*(5), 5930–5939.

Zhu, T., Ma, Q., Zhang, S., & Liu, Y. (2014). Context-free attacks using keyboard acoustic emanations. In *Proceedings of 2014 ACM SIGSAC conference on computer and communication security—CCS '14*, *3(1)*, 453–464.